# MPEG-2 变长码域实时视频水印*)

邹复好　卢正鼎　凌贺飞
(华中科技大学计算机学院　武汉 430074)

**摘　要**　通常,同公有水印算法相比,私有水印算法表现出更好的性能。产生这种结果的原因是,在水印检测时,私有数字水印算法可以借助原始载体作为参照点,对检测载体相对于原始载体的变化量做准确的计算。在公有算法中,如何在没有原始载体的情况下,寻找一个稳定参照点是提高水印性能的关键。本文提出的公有视频水印算法是利用扩展 m-序的良好均衡性产生稳定的参照点,从而大大提高水印系统的性能。考虑视频水印的实时性要求,即尽量避免一些计算复杂性较高的操作(如 DCT 变换和运动补偿等操作),水印的嵌入和检测过程均在变长码域进行。为了防止视觉质量严重退化,在水印嵌入时采用人眼视觉模型来控制修改幅度。同 Lu 和 Frank 等提出的视频水印算法相比,在保证较好的视觉质量和实时性前提下,本文提出的视频水印算法有更好的鲁棒性。

**关键词**　视频水印,实时,变长码域,扩展 m-序

## Real-time MPEG-2 Video Watermarking in the VLC Domain

ZOU Fu-Hao　LU Zheng-Ding　LING He-Fei
(College of Computer Science & Technology, Huazhong University of Science & Technology, Wuhan 430074)

**Abstract**　Comparing with the public watermarking scheme, the private watermarking scheme's better performances consist in that original host is exploited as a reference point to compute modification amount during watermarking detection. Among these public watermarking schemes, how to search a stable reference point without resorting to original host is a key issue of improvement the performances of watermarking system. The proposed scheme exploits the balance property of extended m-sequence adequately to generate a stable reference point and obtains greatly improving of watermarking performance. Considering the real-time requirement of video watermarking, the processes of the watermarking embedding and detecting are directly performed in the VLC domain to avoid some computationally expensive operations(i. e. DCT, inverse DCT and motion compensating). To prevent from visual quality degradation, the human visual system(HVS) is used to control the modification strength. Under the premise of assuring better visual quality and real-time property, this scheme is more robust than the scheme proposed by Lu and Frank et al.

**Keywords**　Video watermarking, Real-time, Variable length codeword, Extended m-sequence

## 1　引言

随着多媒体技术和互联网技术的发展,数字作品的复制、分发和传播变得更加便捷,这在给人们带来便利的同时,也给一些非法复制和散布数字产品者带来可乘之机。因此,如何对数字产品实施更加有效的版权保护,是促进数字化技术进步的一个重要因素。目前,数字水印技术成为多媒体版权保护的一项重要技术。在现存的水印研究文献中,图像水印远多于视频水印。然而,在实际应用中,视频信息更加有用,因而需要以更高优先级加以保护。尽管现有的部分图像水印算法可以直接扩展到视频应用中,然而视频水印除了满足图像水印的一些基本要求(如感知透明性、鲁棒性等)以外,还要满足一些特殊要求,如盲检测、实时性、维持恒定比特率。

近年来,一些视频水印算法被提出[1~5],这些视频水印算法或者在原始视频[1]中嵌入水印,或者在压缩域[1~5]中嵌入水印。通常,视频序列是以压缩格式存放,因而压缩域视频水印更实际些。在文[1]中,Hartung 和 Girod 提出一种 DCT 系数域的基于扩展频谱思想的公有视频水印算法。他们把水印模式调制成一个与视频帧尺寸相同的二维数组,对该二维数组进行 8×8 分块 DCT 变换后,叠加到视频帧的 DCT 系数上;在水印嵌入之前,需要一些额外的操作,如:逆熵编码、反"之"字形扫描和反量化;水印检测时,需要完全解码到空域,因而计算复杂性比较高。并且基于扩展频谱的公有水印算法,水印检测的前提条件是水印模式和载体之间的相关性为零。通常这个假设在小样本情况下很难成立,所以水印的鲁棒性比较差。

在文[2,3]中,Langelaar 等提出了一种运行在量化 DCT 系数域的差分能量水印算法。在该算法中,以 8×8DCT 块为基本单位,'I'帧的亮度空间被分成一序列等长的区域,每一区域又分两个相同大小的子区域。首先,每个区域中的一个截断索引(表示 DCT 块中"之"字形扫描后的 DCT 系数位置,用于平衡水印的鲁棒性和感知透明性)常量被确定;然后,根据截断索引计算子区域的能量;水印嵌入是通过设置其中一个子区域的能量为零(即该子区域截断索引之后的高频系数

*)信息产业部资助的电子信息产业发展基金项目(2004-2006);科技部资助的科技型中小企业创新基金项目(04C26214201284)。**邹复好**　在读博士,主要研究领域为信息安全、数字水印、图像加密;**卢正鼎**　硕士,教授,主要研究领域为信息安全、分布异构系统集成;**凌贺飞**　博士,讲师,主要研究领域为图像处理、数字水印。

被移除)。作者声称该算法在不造成视觉退化的前提下是无法移除水印信号的;然而,这种算法致命的缺陷是,既然可以通过移除一个子区域的高频系数的方法嵌入水印,攻击者也可以在不会造成视觉失真的前提下移除另外一个子区域的高频系数,这样该算法就很难抵抗低通滤波攻击。在文[4]中,Ling 等提出一种变长码域差分数字水印算法,同差分能量算法相比,前者更加实时。由于差分数字水印算法嵌入原理和差分能量基本相同,因而对低通滤波攻击也十分敏感。

在文[5]中,Lu 等提出一种基于均值过滤的变长码域实时视频水印算法。其水印模式是一个零均值、单位方差的高斯噪声序列,其长度与嵌入区域的宏块个数相同(即每一个宏块嵌入一位)。水印嵌入时,如果与当前宏块对应的水印信号符号为正,则该宏块内所有行程码层次加 1,否则减 1;水印检测时,根据宏块中所有行程码层次均值与整个嵌入区域的行程码层次均值的差值,确定对应位水印信号值,然后根据检测到的水印与原始水印归一化相关值,确定水印是否存在。在该算法中,在水印嵌入时,为了避免视频编码和解码操作,如果调制后的行程码没有对应的变长码字,则寻找一个与当前行程码层次值最近的一个变长码代替;而且,为了避免视觉失真,如果调制后的行程码的层次值小于或等于零,则该行程码层次设置为 1。这样,约 20%～30%宏块中的变长码不能实现有效嵌入,相应地,其检测响应值比较低,因而该水印算法的鲁棒性较差。

上述算法是目前视频水印研究领域中比较典型的视频水印算法。从上述回顾中,不难发现这些算法在实时性、感知透明性和维持恒定比特率等方面基本上都能满足视频水印的要求,但鲁棒性还需要进一步加强。本文的目标就是提出一种比上述算法更加鲁棒的公有实时视频水印算法,水印嵌入直接运行在变长码域,水印嵌入和检测之前只需要逆熵编码,因而可以满足实时性要求;水印模式为扩展的 m-序,其良好的均衡性能被用于产生稳定的参照点,借助于该参照点可以准确计算修改幅度;同时视觉感知模型被引入控制水印嵌入强度,可以在不造成视觉失真的前提下,获得最大鲁棒性。本文组织如下:第 2 节中给出水印算法;第 3 节以理论推导的方式给出误警率计算方法,并用其计算检测阈值;第 4 节给出同 Frank[1] 和 Lu[5] 等提出的算法相比较的实验结果,实验证实该算法满足实时性和感知透明性前提下,有更好的鲁棒性;最后给出结论和未来工作展望。

## 2 变长码域视频水印

本文所讨论的视频水印算法主要是针对 MPEG-2 压缩格式的视频水印。2.1 节简单介绍 MPEG-2 压缩标准,并阐明水印的嵌入位置和为什么可以满足实时性要求;在 2.2 和 2.3 节详细描述水印算法,并给出恒定位率控制措施。

### 2.1 水印嵌入位置选择

为了实现在压缩数据中嵌入水印,必须考虑 MPEG-2 压缩格式。在介绍水印算法之前,简单描述 MPEG-2 视频压缩标准[ISO96]。MPEG-2 视频流在语法上是分层表示的,每一层包含一个或多个子层,如图 1 所示。一个视频序列由多个图像组(GOP-group of picture)组成,图像组包含连续的视频帧,如'I','B','P'帧;每一帧分为多个切片(slice)和宏块(macro-block)。最低层是块层(block-layer)。一个宏块由亮度和色度块组成,在色度格式为 4∶2∶0 的一个宏块中有 4 个亮度块(Y0,Y1,Y2,Y3)和 2 个色度块(Cb,Cr)。

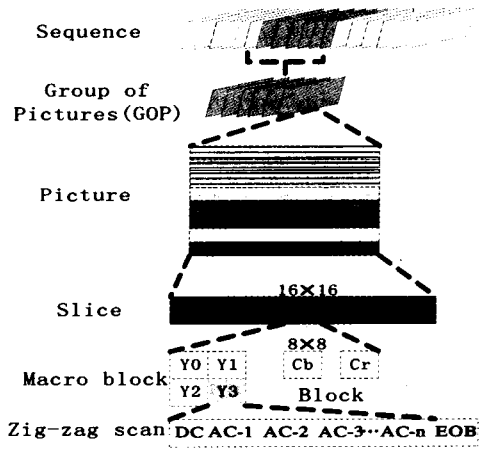



图 1 MPEG-2 视频流分层语法表示(色度格式 4:2:0)

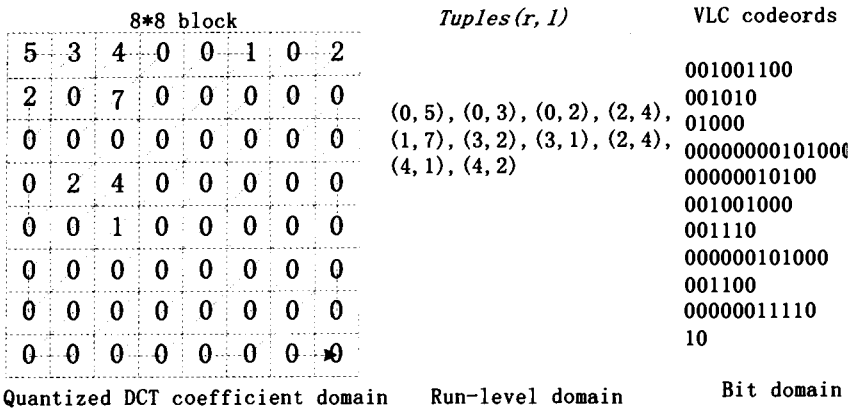



图 2 块层中的不同域表示

在块层中,空间中的 8×8 的像素块用 64 个量化的 DCT 系数表示,图 2 表示块层中根据解码顺序分成了 3 个域,第一个域是量化后的 DCT 系数域(quantized DCT coefficient domain),块中包含 8×8 个整数项,其对应量化后的 64 个 DCT 系数大部分为零,特别是空间中高频部分;在行程域(run-level domain),也称变长码域(variable length codeword-VLC domain),非零的 AC 系数按"之"字形扫描,然后用一二元组表示为$(r,l)$,其中 $r$ 是当前系数之前零的个数,$l$ 等于系数值。块层的最低层域是位域,是对元组$(r,l)$进行熵编码后得到变成码码字,每一块的结尾的码字是块结束(EOB-end of block)

标志。

用于 MPEG-2 压缩视频的实时视频水印应该紧密结合 MPEG-2 压缩标准，以避免计算复杂性操作，如 DCT、逆 DCT 和运动补偿等操作。本文的视频水印算法运行在变长码域，嵌入水印前只需要变长码解码和行程码解码。水印嵌入的基本过程如图 3 所示。

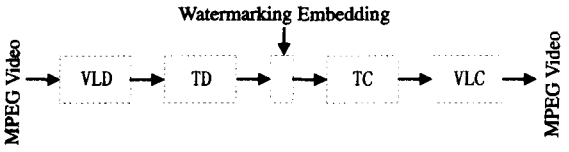



图 3　变长码域水印思想

在 MPEG-2 视频序列中，'P'帧和'B'帧数据是相对于参考帧的预测差值，对'P'帧和'B'帧的修改会产生更大的视觉误差，进而造成严重视觉退化。本算法的水印嵌入是通过对'I'帧亮度空间的直流系数进行细微修改。选择亮度空间的原因是：视频流经常会改变位率存储或传输，若选择色度空间则会由于色度各式变化产生同步问题。选择直流系数原因是：水印嵌入操作是对行程码的层次值 $l$ 进行细微修改，这样一方面避免由于交流系数层次值的修改影响后续码字的重新编码（如果选择 AC 系数就可能出现这种问题），另外一方面把水印嵌入在感知最重要的部位，可以提高水印算法鲁棒性。该思想在文[7,8]也提到。在文[8]中，Huang 等用定量分析的方法阐明选择直流系数作为嵌入空间的合理性。

### 2.2　水印嵌入算法

水印模式为扩展 $m$ 序，选择扩展 $m$ 序作为水印模式的一个原因是其周期值为偶数，这样硬件实现时便于产生一个时钟周期为偶数的信号；另一个原因是其良好的平衡性，以取值为{−1,1}的扩展 $m$ 序为例，其周期为 $2^n$，$n\in Z$，其均衡表现在：

$$\sum_{i=1}^{2^n} w(i)=0 \tag{1}$$

利用该特性可以产生稳定的参考点。参考点的稳定性将在水印检测部分详细讨论。

'I'帧的亮度空间以 8×8DCT 块为单位划分成若干区域，在每一个区域中嵌入一个水印模式。根据水印模式的长度将每一区域划分成相应数量的子区域，即在每一子区域中嵌入水印模式的一位。假定 $(r_{ij},l_{ij})$ 表示当前区域的第 $i$ 个子区域的第 $j$ 个 8×8DCT 块的 DC 系数所对应的行程码，则该区域所有直流系数的行程码层次绝对值之和为：

$$S_i=\sum_{j=1}^{L_{sub\_rg}} |l_{ij}| \tag{2}$$

其中 $L_{sub\_rg}$ 表示子区间 8×8DCT 的块数。序列 $S=\{S_i,1\leqslant i\leqslant 2^n\}$ 的均值为：

$$u=\frac{1}{2^n}\sum_{i=1}^{2^n} S_i \tag{3}$$

这里根据 $w(i)$ 的取值，调整第 $i$ 个子区域直流系数的行程码层次绝对值之和，满足如下关系：

$$S_i^h=\begin{cases} u+T, \text{if } w(i)=1 \\ u-T, \text{if } w(i)=-1 \end{cases}, \text{即 } S_i^h=u+w(i)\cdot T \tag{4}$$

$T$ 的选择如下：

$$\text{Min}_T=\min\{|S_1-u|,\cdots,|S_{2^n}-u|\},\ \text{Max}_T=\max\{|S_1-u|,\cdots,|S_{2^n}-u|\}$$

$$T=\lambda\cdot\text{Min}_T+(1-\lambda)\cdot\text{Max}_T,\ 0\leqslant\lambda\leqslant 1 \tag{5}$$

其中 $\lambda$ 为调节因子，当 $\lambda=1$ 时获得最小失真同时鲁棒性最低；当 $\lambda=0$ 时获得最大鲁棒性同时保真度最差。根据 $S_i,S_i^h$ 之间的关系，对每一行程码分别调制。调制策略可分为正调制（positive modulation-PM）和负调制（negative modulation-NM），如图 4 所示。

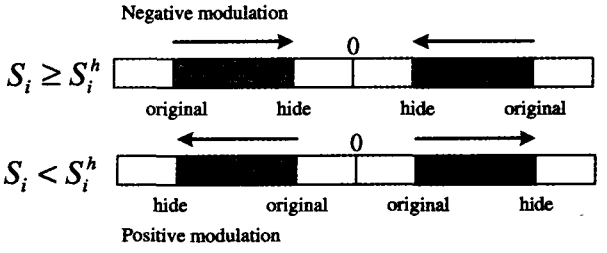



图 4　根据 $S_i,S_i^h$ 和之间的关系，两种不同的调制策略

以第 $i$ 个子区间中的第 $j$ 个直流系数所对应的行程码 $(r_{ij},l_{ij})$ 为例，在正、负调制情况下，层次 $l_{ij}$ 的调制如下：

$$l_{ij}^h=\begin{cases} l_{ij}+\text{sign}(l_{ij})\cdot|S_i^h-S_i|\cdot\dfrac{JND_{ij}}{\sum_{j=1}^{L_{sub\_rg}} JND_{ij}}, PM \\ l_{ij}-\text{sign}(l_{ij})\cdot|S_i^h-S_i|\cdot\dfrac{JND_{ij}}{\sum_{j=1}^{L_{sub\_rg}} JND_{ij}}, PM \end{cases} \tag{6}$$

其中 sign(·)为符号函数，$JND_{ij}$ 表示根据 Watson 视觉模型[9]计算出的层次 $l_{ij}$ 允许修改的最大量。由于修改的是 DC 系数，即 $l_{ij}$ 的修改不影响 $r_{ij}$ 取值，故修改后的 $(r_{ij},l_{ij})$ 行程码为 $(r_{ij},l_{ij}^h)$。

### 2.3　水印检测算法

通常，嵌入水印后的视频序列会遭受一些攻击。根据攻击性质可分为无意攻击（如通常的一些信号处理）和恶意攻击（以破坏和篡改水印为目的）。为了便于分析，假定待检测的视频是没有遭受任何攻击的视频序列。依照水印嵌入过程，将视频的'I'帧以 8×8DCT 块为单位，划分多个区域。然后对每一区域又划分等长的子区域，对某一特定区域，计算该区域所有子区域的直流系数的行程码层次绝对值之和 $S_i^e$ 及均值 $u^e$：

$$u^e=\frac{1}{2^n}\sum_{i=1}^{2^n} S_i^e=\frac{1}{2^n}\sum_{i=1}^{2^n} S_i^h=\frac{1}{2^n}\sum_{i=1}^{2^n}(u+w(i)\cdot T)=\frac{1}{2^n}\sum_{i=1}^{2^n} u+\frac{1}{2^n}w(i)\cdot T=u+0=u \tag{7}$$

从式(7)中不难发现，在水印嵌入前后，均值点没有发生改变。在水印嵌入和检测过程中，该均值点作为参照点。从表达式 $u^e=u$ 可以看出，该参照点是稳定的。在公有水印方案中，稳定的参照点有助于提高水印系统的鲁棒性。这里依据 $S_i^e$ 与 $u^e$ 的大小关系，可以检测出水印信号 $W^e=\{w^f(i),1\leqslant i\leqslant 2^n\}$，$w^f(i)$ 的取值为：

$$w^f(i)=bipolar(S_i^e-u^e) \tag{8}$$

其中函数 $bipolar(\cdot)$ 可以定义为：

$$bipolar(t)=\begin{cases} 1, \text{if } t\geqslant 0 \\ -1, \text{if } t<0 \end{cases} \tag{9}$$

然后计算检测的水印 $W^e$ 和原始水印 $W$ 的相关系数：

$$\rho(W,W^e)=\frac{\sum_i w(i)\cdot w^f(i)}{\sqrt{\sum_i w^2(i)}\sqrt{\sum_i (w^f(i))^2}} \tag{10}$$

根据相关系数 $\rho(W,W^e)$ 取值与检测阈值 Threshold 之间的关系，确定水印是否存在。详细判别如下：

$$\begin{cases}\text{existing watermark}, \rho(W,W^e)\geqslant \text{Threshold}_e \\ \text{without watermark}, \rho(W,W^e)<\text{Threshold}_e\end{cases} \tag{11}$$

由于视频序列的大小在水印嵌入过程不允许改变，即维持恒定的位率。因此在水印嵌入过程中，采取专门的措施来维持恒定的位率。这里统计修改前所有的变长码长度和修改之后所有变长码长度之差。如果尺寸变小，则在切片之间插入相应数量的比特，否则通过删除一些纹理比较丰富的区域的高频系数，这样基本上就可以维持恒定的位率。

## 3 误警率和检测阈值的计算

通常，误警率(probability of false positive)表示在没有水印的作品中检测出水印的概率，借助误警率的值可以求解水印检测的阈值。在现有的误警率求解方法中，一些是通过概率统计方法进行求解。采用统计的方法需要进行大量的实验，不便于实施。这里用理论推导的方法求解误警率值。误警率定义如下：

$$P_{fp}=P\{\rho(W,W^e)\geqslant \text{Threshold}_e \mid \text{without watermark}\} \tag{12}$$

其中 $P\{A|B\}$ 是事件 $B$ 发生的情况下事件 $A$ 发生的概率。在式(10)中，由于 $w(i)$ 和 $wf(i)$ 或者为 1，或者为 $-1$，则 $w^2(i)=(wf(i))^2=1$，则式(10)可重新表示为：

$$\rho(W,W^e)=\frac{\sum_i w(i)\cdot wf(i)}{\sqrt{\sum_i w^2(i)}\sqrt{\sum_i (wf(i))^2}}=\frac{\sum_i w(i)\cdot wf(i)}{N_w} \tag{13}$$

其中 $N_w$ 为水印 $W$ 的长度，即 $N_w=2^n$。

用 $P_E$ 表示水印检测时的位错率。当 $w(i)\neq wf(i)$(即 $w(i)=-wf(i)$)时，发生位错。假定有 $k(i)=w(i)\cdot wf(i)$，如果 $k(i)=-1$，表示一位发生错误；$k(i)=1$，表示没有错误发生。把 $k(i)$ 分别代入式(12)和(13)，则有：

$$P_{fp}=\{\sum_i k(i)\geqslant N_w\cdot \text{Threshold}_e \mid \text{without watermark}\} \tag{14}$$

和

$$\rho(W,W^e)=\frac{\sum_i k(i)}{N_w} \tag{15}$$

既然 $k(i)\in\{-1,1\}$，不难推出 $\sum_i k(i)$ 的值一定来自于集合 $\{-N_w,-N_w+2,-N_w+4,\cdots,N_w-4,N_w-2,N_w\}$(即 $\sum_i k(i)=-N_w+2m, m=0,1,\cdots,N_w$)，于是可以得出：

$$P_{fp}=\{\sum_i k(i)\geqslant N_w\cdot \text{Threshold}_e \mid \text{without watermark}\}=\sum_{m=\lceil N_w\cdot(\text{Threshold}_e+1)/2\rceil}^{N_w} P\{\sum_i k(i)=-N_w+2m \mid \text{without watermark}\} \tag{16}$$

其中 $P\{\sum_i k(i)=-N_w+2m \mid \text{without watermark}\}$ 是序列 $\{k(i)\}$ 包含 $m$ 个 1 和 $N_w-m$ 个 $-1$ 的概率。于是有：

$$P\{\sum_i k(i)=-N_w+2m \mid \text{without watermark}\}=\binom{N_w}{m}P_E^{N_w-m}(1-P_E)^m \tag{17}$$

其中 $P_E$ 是 $k(i)=-1$ 的概率，$\binom{N_w}{m}=\frac{N_w}{M!\ (N_w-m)!}$。既然没有水印嵌入，便可以假定检测的水印 $wf(i)$ 是独立同分布的，则可以认为 $P_E=0.5$。代入式(16)和(17)可以得出：

$$P_{fp}=\sum_{m=\lceil N_w\cdot(\text{Threshold}_e+1)/2\rceil}^{N_w}\binom{N_w}{m}0.5^{N_w} \tag{18}$$

通常，给定了期望的误警率，通过式(18)可以确定水印检测阈值 $\text{Threshold}_e$。对于固定的检测阈值，随着水印长度增加，误警率降低。类似地，增加水印长度可以降低虚警概率。检测阈值 $\text{Threshold}_e$ 的确定应该合理权衡误警率和虚警率之间的关系，阈值越大，误警率越小，但是虚警率就越大。在给定误警率为 $10^{-6}$ 情况下，计算的监测阈值为 0.1359。

## 4 算法实现和实验结果分析

为了评价本算法的性能，这里选择同 Frank[1] 和 Lu[5] 等提出的视频水印算法进行比较。选择这两种算法的主要原因有：(1)在目前水印攻击研究文献中，除几何攻击以外，还没有一种攻击对上述两种算法是致命的，而 DEW[2,3] 算法惧怕低通滤波攻击；(2)这两种算法是视频水印领域比较经典的两个算法。测试视频选取的是著名的'flower-garden'视频序列，该视频序列的视频帧尺寸为 352×240，共有 150 个视频帧，其中有 26 个'I'帧，25 个'P'帧，99 个'B'帧，位率为 8Mbit/s。在水印嵌入时，参数的选取对水印性能影响很大。为了公正客观地评价上述算法的性能，要求在每一个'I'帧中嵌入一个水印模式，调整水印嵌入参数使得每一帧的水印检测响应值为一固定值，本实验设定检测响应值为 0.95；然后分别在视觉质量、鲁棒性和实时性 3 个主要方面对算法性能进行评判。

### 4.1 视觉质量评价

通常，嵌入水印后的视频相对于原始视频是否有明显视觉质量退化，是通过计算 *PSNR* 值来进行评价的，其表达式为 $PSNR=MN^{\max I^2_{m,n}}/\sum_{m,n}(I_{m,n}-\bar{I}_{m,n})$，其中视频帧尺寸为 $M\times N$，$I_{m,n}$ 为原始帧位置为 $(m,n)$ 处像素值，$\bar{I}_{m,n}$ 为嵌入水印后视频帧位置为 $(m,n)$ 处的像素值。通常 *PSNR* 值越大，视觉质量越好。这里计算用上述 3 种算法分别嵌入水印后的视频相对于原始视频帧的 *PSNR* 值。在图 5 中，*X*-轴表示'*I*'帧的序号，*Y*-轴表示的是 *PSNR* 值。从图 5 中可以看出，本算法在所有帧上的 *PSNR* 值均高于其他两种算法。该结果表明，在获得同样的检测响应值情况下，本算法对载体的修改幅度最小，因而有较好的视觉质量。同时发现，其它两种算法的 *PSNR* 值折线比较平，反映这两种算法对载体的修改并没根据载体的内容确定嵌入强度。

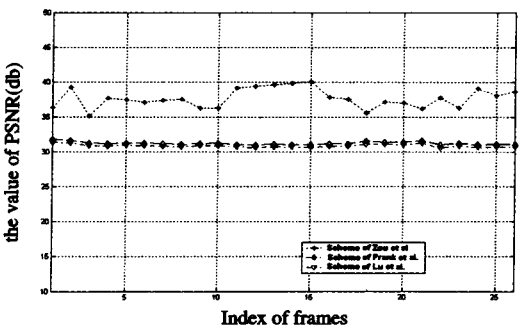



图 5 三种不同算法对视频序列'flower-garden'添加水印后的 PSNR 值

### 4.2 鲁棒性评价

为了测试 3 种算法的鲁棒性，这里分别对用上述 3 种算法嵌入水印后的视频进行一些常用的攻击，如 MPEG 压缩攻击(即对 8Mbit/s 的视频嵌入水印后以更低的位率重新编码，编码位率分别为 6Mbit/s、4Mbit/s、2Mbit/s)、低通滤波攻击、

中值过滤攻击、高斯噪声攻击、高斯过滤攻击、锐化攻击和随机弯曲攻击后的检测响应值

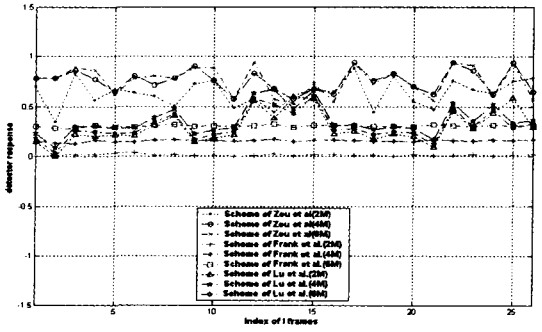


图 6　以 6Mbit/s,4Mbit/s,2Mbit/s 压缩攻击后的检测响应值

机弯曲攻击。从攻击后的视频检测水印，计算检测响应值。比较 3 种算法对同一种攻击视频中获得的检测响应值，来判断它们的鲁棒性。通常检测响应值越大，鲁棒性越好。图 6 是压缩攻击的结果，图 7(a)～(f)分别是低通滤波攻击、中值过滤攻击、高斯噪声攻击、高斯过滤攻击、锐化攻击和随机弯曲攻击的结果。从图 6 和图 7 中可以看出，本算法在所有攻击视频的检测响应值都高于另外两个算法，表明本算法的鲁棒性更好。

### 4.3　实时性评价

为了证实本算法可以实现水印的实时嵌入和检测，这里比较对视频序列'flower-garden'实施以下 8 种不同操作的耗时，如图 8 所示。在图 8 中，横轴代表操作的编号，纵轴表示进行该种操作耗费的时间。这 8 种操作分别为：(1)MPEG-2 编码格式视频序列完全解码到空域然后又重新编码所使用的时间，一般的空域嵌入算法时间和此时间比较相近；(2)用 Zou 的算法嵌入水印耗时；(3)用 Zou 的算法检测水印耗时；(4)用 Lu 的算法嵌入水印耗时；(5)用 Lu 的算法检测水印耗时；(6)用 Frank 的算法嵌入水印耗时；(7)用 Frank 的算法检测水印耗时；(8)单纯解码到 VLC 域耗时。从图 8 中可以看出，操作(2)～(7)中，除了操作(7)(检测水印在空域中进行)以外，其它 5 种操作和操作(8)耗时比较接近，表明该算法能够满足实时性要求。

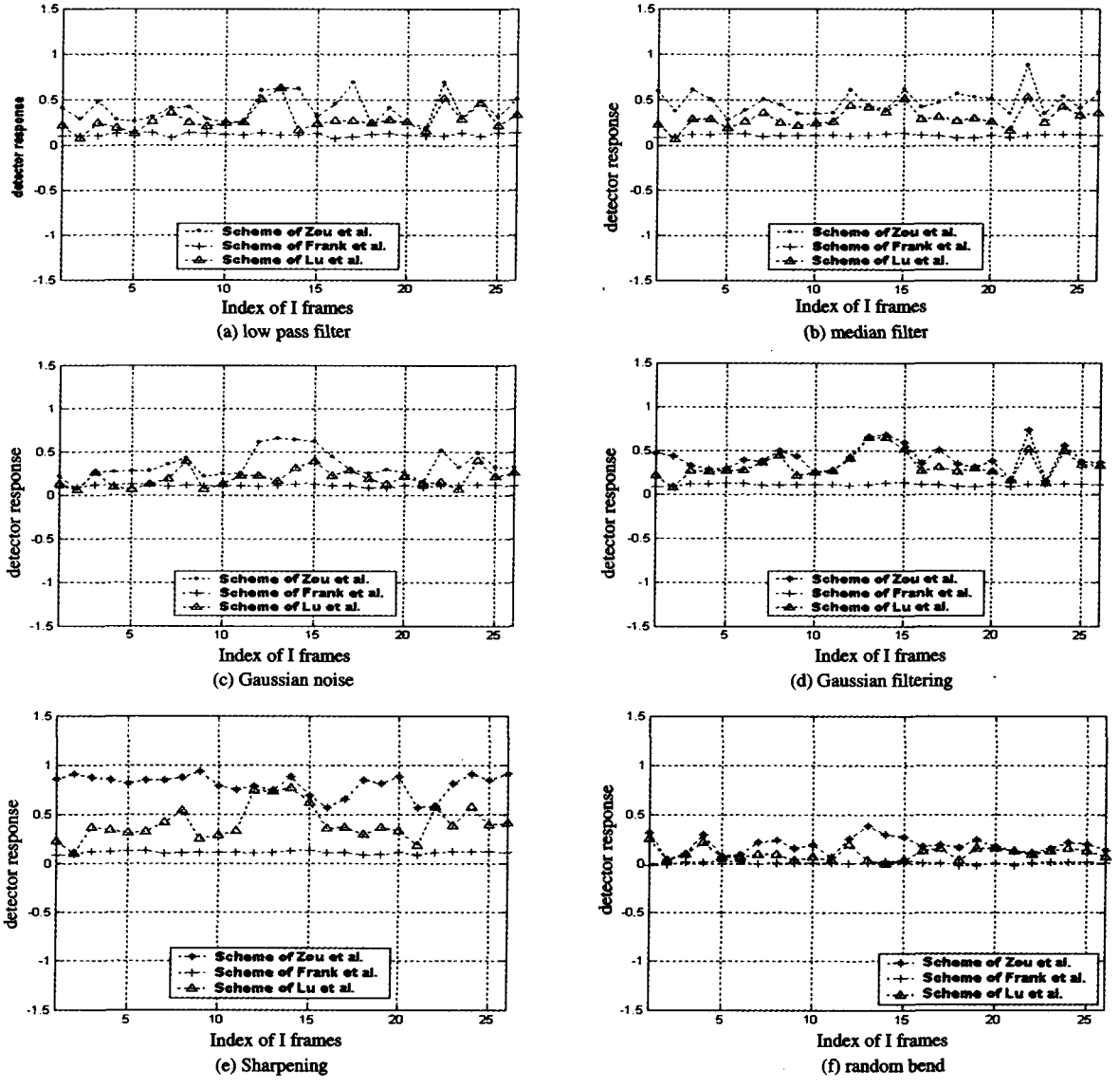
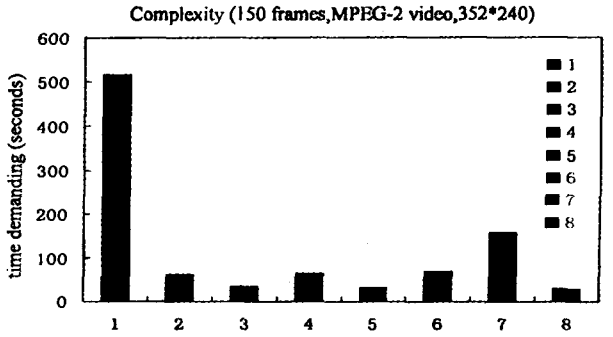



图 7　低通滤波攻击、中值过滤攻击、高斯噪声攻击、高斯过滤攻击、锐化攻击和随机弯曲攻击等攻击后的检测响应值




1:完全解码和编码;2:Zou 的水印嵌入耗时;3:Zou 的水印检测耗时;4:Lu 的水印嵌入耗时;5:Lu 的水印检测耗时;6:Frank 的水印嵌入耗时;7:Frank 的水印检测耗时;8:解码到 VLC 域耗时

图 8 时间消耗比较

**结论和未来展望** 本文提出了一个使用扩展的 m-序作为水印模式的变长码域的实时视频水印算法。通过理论分析和试验验证表明,该算法在满足实时性和视频水印其它基本要求的前提下,同 Lu 和 Frank 提出的两种算法进行比较,能够获得更好鲁棒性,同时引起的视觉退化最小,即本算法性能更好。

本算法选用扩展的 m-序作为水印模式,充分利用其良好的均衡性获得了较好的性能。由于扩展 m-序有较好的自相关特性和交叉相关特性,利用该特性和码分复用技术可以提高水印系统的有效载荷,这将是以后进一步研究的内容。

## 参 考 文 献


1 Frank H, Bernd G. Watermarking of uncompressed and compressed video. Signal Processing, 1998, 66(3): 283～301

2 Langelaar G C, Lagendijk R L, Biemond J. Real-time labeling of MPEG-2 compressed video. Journal of Visual Communication and Image Representation, 1998, 9(4): 256～270

3 Langelaar G C, Lagendijk R L. Optimal differential energy watermarking of DCT encoded images and video. IEEE Transactions on Image Processing, 2001, 10(1): 148～158

4 Ling Hefei, Lu Zhengding, Zou Fuhao. New real-time watermarking algorithm for compressed video in VLC domain. In: Proc. of 2004 International Conference on Image Processing(ICIP). Piscataway, NJ, USA: IEEE, 2004. 2171～2174

5 Lu Chun-Shien, Chen Jan-Ru, Liao H-Y M, et al. Real-time MPEG video watermarking in the VLC domain. In: Proc. of 16th International Conference on Pattern Recognition. Los Alamitos, CA, USA: IEEE Comput. Soc, 2002. 552～555

6 Lu Chun-Shien, Huang Shih-Kun, Sze Chwen-Jye, et al. Cocktail watermarking for digital image protection. IEEE Transactions on Multimedia, 2000, 2(4): 209～224

7 Cox I J, Kilian J, Leighton F T, et al. Secure spread spectrum watermarking for multimedia. IEEE Transactions on Image Processing, 1997, 6(12): 1673～1687

8 Huang Jiwu, Shi Y Q, Shi Yi. Embedding image watermarks in DC components. IEEE Transactions on Circuits and Systems for Video Technology, 2000, 10(6): 974～979

9 Watson A B. DCT quantization matrices visually optimized for individual images. In: Proc. of Conference of Human Vision, Visual Processing, and Digital Display IV. San Jose, CA, USA: SPIE, 1993. 202～216

10 Zou Fuhao, Lu Zhengding, Ling Hefei. A multiple watermarking algorithm based on CDMA technique. In: Proc. of the 12th ACM International Conference on Multimedia(ACM Multimedia 2004). New York, NY, USA: ACM, 2004. 424～427

11 Fiebig U-C G, Schnell M. Correlation properties of extended m-sequences. Electronics Letters, 1993, 29(20): 1753～1755


(上接第 144 页)

**结论** 超椭圆曲线密码尽管近几年在理论与应用中取得了巨大的进展,新理论、新方法及新技术也不断涌现,但到目前为止尚未形成一个完整的理论体系,仍有许多问题等待解决。本文给出关于一条超椭圆曲线的 jacobian J(K)的快速算法,可以快速有效地计算出超椭圆曲线 Jacobian 除子类群的阶,并通过实例证明该算法的有效性。超椭圆曲线密码体制(HCC)的标准化和实用化是一个亟待解决的问题,我们下一步的研究方向是如何提高超椭圆曲线 Jacobian 上的基本运算及其上标量乘运算的速度,从而使超椭圆曲线密码体制得以实际应用于密码安全方案中。

## 参 考 文 献


1 Koblitz N. Hyperelliptic cryptosystems. Journal of Cryptology, 1989(1): 139～150

2 Hess F, Seroussi G, Smart N. Two Topics in Hyperelliptic Cryptography: [HP Labs Technical Reports, HPL-2000-118]. 2000

3 Adleman L, Huang M. Counting rational points on curves and abelian varieties over finite fields. In ANTS-2, LNCS 1122, Springer-Verlag, 1996. 1～16

4 Pila J. Frobenius maps of abelian varieties and finding roots of unity in finite fields. Math. Comp., 1996, 55(192): 745～763

5 Satoh T. Canonical Lifting of Elliptic Curves and p-Adic Point Counting - Theoretical Background. Workshop on Elliptic Curve Cryptography - ECC'00, 2000. Available at: http://www.exp-math.uni-essen.de/～galbra/eccslides/eccsldes.html

6 Gaudry P, Hess F, Smart N. Constructive and destructive facets of Weil descent on elliptic curves. preprint, January 2000. Available at: http://www.hpl.hp.com/techreports/2000/HPL-2000-10.html

7 Kocher P, Jaffe J, Jun B. Differential power analysis. Advances in Cryptology - Crypto '99, Lecture Notes in Computer Science, Springer-Verlag, 1999, 1666: 388～397

8 Kelsey J, Schneier B, Wagner D, Hall C. Cryptanalytic attacks on pseudorandom number generators. Fast Software Encryption - FSE '98, Lecture Notes in Computer Science, Springer-Verlag, 1998, 1372: 168～188

9 Dobbertin H, Bosselaers A, Preneel B. RIPEMD-160: A strengthened version of RIPEMD. Fast Software Encryption - FSE '96, Lecture Notes in Computer Science, Springer-Verlag, 1996, 1039: 71～82

10 Vaudenay S. Hidden collisions on DSS, Advances in Cryptology - Crypto '96, Lecture Notes in Computer Science, Springer-Verlag, 1996, 1109: 83～88

11 Blake-Wilson S, Menezes A. Unknown key-share attacks on the station-to-station(STS) protocol. Public Key Cryptography - Proceedings of PKC '99, Lecture Notes in Computer Science, Springer=Verlag, 1560: 154～170

12 Kocher P. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems, Advances in Cryptology - Crypto '96, Lecture Notes in Computer Science, Springer-Verlag, 1996, 1109: 104～113

13 张方国,王育民. 超椭圆曲线密码体制的研究与进展. 电子学报, 2002, 30(1): 26～131